Mary L. Russell (NJ-0525119955)
Roberta D. Liebenberg (*pro hac vice* application forthcoming)
Gerard A. Dever (*pro hac vice* application forthcoming)
FINE, KAPLAN AND BLACK, R.P.C.
One South Broad Street, 23rd Floor
Philadelphia, PA 19107
Tel: (215) 567-6565
mrussell@finekaplan.com
rliebenberg@finekaplan.com
gdever@finekaplan.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

JORGE FERNANDEZ, Plaintiff, v. SAMSUNG ELECTRONICS AMERICA, INC., Defendant	Civil Action No. **COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiff Jorge Fernandez ("Plaintiff"), a resident of Florida, individually and on behalf of all others similarly situated, through the undersigned counsel below, hereby alleges the following against Defendant Samsung Electronics America, Inc., 85 Challenger Road, Ridgefield, New Jersey 07660-2118 ("Samsung" or "Defendant"). Based upon personal knowledge as to his own actions, and upon information, belief and investigation of counsel as to all other matters, Plaintiff specifically alleges as follows:

SUMMARY OF THE CASE

1. Plaintiff brings this class action on behalf of a nationwide class and a Florida sub-class (together, the "Classes") against Samsung Electronics America, Inc. ("Samsung" or

"Defendant") for its failure to properly secure and safeguard the sensitive and confidential personally identifiable information, including names, addresses, telephone numbers, email addresses, dates of birth and other sensitive information (collectively, "personally identifiable information" or "PII"), of millions of its current and former customers ("Class Members).

2. In July 2022, a large quantity of PII entrusted to Samsung by its customers was exfiltrated and stolen by an unauthorized third party (the "Data Breach"). Only a few months earlier, in March 2022, Samsung had confirmed another data security breach; at that time, an organization called Lapsus$ accessed and stole Samsung's confidential data and published 190GBs of Samsung's confidential data online.

3. Despite this earlier breach and knowledge of the exposed sensitive technical data and the immediate need to protect customers' PII from attackers, Samsung utterly failed to adequately secure its systems and allowed another breach to occur, this time compromising consumer PII.

4. Plaintiff and Class Members entrusted Samsung with their sensitive and valuable PII. Even more egregious, there was ***absolutely no need*** for Samsung to collect this PII from purchasers of its electronic devices or other appliances. Samsung did so to increase its profits, to gather information regarding its customers to be able to track its customers and their behaviors, and to use the data for its own benefit and purposes.

5. Plaintiff and Class Members could not have expected that purchasing an electronic device or home appliance and registering for an account in connection with the purchase, which was required by Samsung to access features of the devices, would lead to such a devastating loss and continuing risk of injury for years following the purchase.

6. By collecting, using, selling, monitoring, and trafficking Plaintiff's and other Class Members' PII for its own economic benefit, and utterly failing to protect it, including by maintaining inadequate security systems, failing to properly archive the PII, allowing access by third parties and failing to implement sufficient security measures, Samsung has caused harm to Plaintiff and Class Members.

7. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct constitutes negligence that proximately caused damages to Plaintiff and Class Members as alleged herein.

8. Samsung disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded; failing to take available steps to prevent unauthorized disclosure of data; and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

9. Alternatively, Defendant has been unjustly enriched. The amounts Plaintiff and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiff's and Class Members' PII. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members

because Defendant failed to implement the data management and security measures mandated by industry standards.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII, a form of property that Samsung obtained from Plaintiff and Class Members; (ii) increased out-of-pocket expenses associated with identity defense, credit monitoring services and other prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 and Florida Deceptive and Unfair Trade Practices Act, § 501.201 *et seq.*; (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; and (vi) violation of Plaintiff's and Class Members' privacy rights.

11. As a direct and proximate result of Samsung's breach of confidence and failure to protect the PII, Plaintiff and Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuses of their PII; ongoing monetary loss and economic harm; loss of value of privacy and confidentiality of the stolen PII; illegal sales of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expenses and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time and

other injuries. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff is a citizen of Florida (and the proposed class members are from various states) while Defendant is a citizen of New York and New Jersey; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

13. This Court has personal jurisdiction over Defendant because Defendant is headquartered in New Jersey and does business in and throughout New Jersey, and the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues. Samsung has intentionally availed itself of this jurisdiction by marketing and selling its products and services in New Jersey.

14. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Ridgefield, New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

THE PARTIES

15. Plaintiff Jorge Fernandez is a citizen and resident of the State of Florida and is a current Samsung customer who had his PII exfiltrated and compromised in the Data Breach.

16. Plaintiff Fernandez purchased a Samsung 70-inch 6900 series television on or about September 24, 2020 and registered online for a Samsung Account, where he submitted his PII to Samsung, including his name, email, date of birth, and zip code.

17. In making his decision to create a Samsung account to gain full access to the product's features, Plaintiff Fernandez reasonably expected that Samsung would safeguard his PII.

18. Plaintiff Fernandez was notified by Samsung on September 2, 2022 by email that Samsung had "recently discovered a cybersecurity incident" that affected some of his personally identifiable information.

19. The email notice of the Data Breach to Plaintiff Fernandez was sent from the address samsung@innovations.samsungusa.com by Samsung Electronics America, Inc., 85 Challenger Road, Ridgefield Park, NJ 07660.

20. Samsung disclosed in the email to Mr. Fernandez that "[i]n late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems" and on or around August 4, 2022, Samsung had determined that "personal information of certain customers was affected." Samsung determined the affected information included "name, contact and demographic information, date of birth, and product registration information" and the information affected could vary for each relevant customer, including Mr. Fernandez.

21. Mr. Fernandez was further instructed by the Samsung notice of the Data Breach that he could check his credit report and "you are entitled under U.S. law to one free credit report annually from each of the three major nationwide credit reporting agencies" and given the contact information for Equifax, Experian and TransUnion.

22. As a direct and proximate result of the Data Breach, Plaintiff Fernandez has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to

conducting research concerning the Data Breach and reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time that Plaintiff Fernandez could have spent on other activities.

23. Plaintiff Fernandez is very concerned about identity theft and the consequences of such theft and fraud resulting from the Samsung Data Breach.

24. Plaintiff Fernandez has spent and will spend a significant amount of time responding to the impacts of the Samsung Data Breach. The time spent dealing with the fallout from the data breach is time that he otherwise would have spent on other activities.

25. As a result of the Samsung Data Breach, Plaintiff Fernandez anticipates spending considerable additional time and money on an ongoing basis to attempt to mitigate and address the harms caused by the Data Breach and will continue to be at increased risk of identity theft and fraud for years to come.

26. Had Plaintiff Fernandez known that the PII Samsung collected would not be safeguarded and would be at risk of a data breach, he would not have purchased the product and would not have created a Samsung account.

27. Samsung is a corporation incorporated in the State of New York, with its United States headquarters and principal place of business located at 85 Challenger Road, Ridgefield, New Jersey 07660-2118.

28. Defendant Samsung Electronics America, Inc. is a United States-based subsidiary of Samsung Electronics Co., Ltd, and is responsible for the production and sale of billions of dollars of electronics sold in the United States.

29. Defendant maintains offices and employees who specifically oversee and handle data privacy, data policies and make data-driven decisions. The Samsung "Privacy Office" is

located at 85 Challenger Road, Ridgefield Park, NJ 07660, NAPrivacy@sea.samsung.com. *See* https://account.samsung.com/membership/terms/privacypolicy.

SAMSUNG'S COLLECTION OF CUSTOMERS' PII FOR SAMSUNG ACCOUNTS

30. Defendant Samsung purports to be an industry leader in technology. It is a technology and electronics giant that sells millions of products and produces over $20 billion of revenue each year. It produces a wide array of electronic devices but is best known for being a top manufacturer of mobile phones, smartphones, televisions, semiconductor chips, tablets, laptops, and home appliances.

31. Samsung's televisions and home appliances connect to the internet and require customers to create a "Samsung Account" prior to accessing many of their device's features. For example, consumers who purchase Samsung "smart" televisions often do so to watch streaming applications such as Netflix or Hulu on a television. An owner of a Samsung smart television cannot access the streaming applications without downloading those applications onto their television. In order to download the applications, the owner of the Samsung smart television must first create a Samsung Account.

32. In fact, for nearly all of its products and services, Samsung requires that the customer create a Samsung Account, forcing customers to entrust Samsung with their PII in order to use the products and services. In fact, regardless of whether the customer purchased a printer, television, smartphone, refrigerator, or laptop, the customer needs to register the products with Samsung to access the features of the devices. Consumers are therefore forced to register accounts; otherwise, many product features are locked and inaccessible. Even using the products in the way they are intended to be used is nearly impossible without the required registration.

33. Samsung requires customers to register the product purchased for warranty-related purposes and to access certain drivers and software needed for the products. These features are essential to the function of the devices.

34. Many features advertised and promoted by Samsung with the sale of the products can only be accessed after the customer creates a Samsung Account. By locking features, making software updates otherwise inaccessible and blocking intended uses of the products, Samsung ensures that nearly every customer who purchases a Samsung product, at some point, will be forced to submit their PII through product registration and creation of the Samsung Account.

35. Other product-related benefits cannot be accessed without a Samsung account. These benefits include, but are not limited to, product support, order tracking, exclusive rewards and offers, Samsung Rewards, Galaxy Store, Samsung Pay, Samsung Health, Samsung Members and Samsung TV Plus.

36. The information collected and stored by Samsung includes, but is not limited to names, dates of birth, mailing addresses, email addresses, phone numbers, precise geolocation data and information about the product the customer purchased.

37. In addition to the information inputted by the customer for the Samsung Account, Samsung also collects still more information automatically from its customers concerning their Samsung devices, such as their mobile network operator; connections to other devices; application usage information; device settings; websites visited; search terms used; which applications, services or features the customer downloaded or purchased; and how and when the applications and services are used.

SAMSUNG PROMISED DATA SECURITY AND PRIVACY

38. Defendant holds itself out as a trustworthy company that recognizes and values the customer's privacy and personal information. Samsung's Privacy Policy for the U.S. assures its customers that Samsung "maintain[s] safeguards designed to protect personal information we obtain through the Services." Samsung represented that it has "industry-leading security" and that "security and privacy are at the core of what we do and what we think about every day."

39. Samsung's privacy policy and online advertisements clearly and unequivocally provide that any personal information provided to Samsung will remain secure and protected. *See* Privacy Notice, Samsung account U.S. Privacy Notice effective September 2, 2022 at https://account.samsung.com/membership/policy/privacy and Privacy Notice, Samsung Privacy Policy for the U.S. last updated October 1, 2021 at https://account.samsung.com/membership/terms/privacypolicy ("We maintain safeguards designed to protect personal information we obtain through the Services.").

40. *See also* https://www.samsung.com/us/privacy/

Samsung's Privacy Principles

Personal information plays a key role in elevating what we do for our community. We engage with it to inform and enhance everything from your experience to our communication, and to create and innovate radical solutions that help you overcome barriers. In this connected, digital age, accessing this information responsibly is more important than ever - clarity and integrity about its use are essential to protecting your privacy and securing your confidence and peace of mind. At Samsung, we prioritize protecting your information, and design our products and services according to our three fundamental Privacy Principles.

Transparency

We tell you the personal information that we collect, how it's used, and how it's shared.

Security

We take data security very seriously. Our products are designed to keep your data private and secure, while always pushing forward to offer you the latest, most groundbreaking innovation.

Choice

As a consumer, you have choices about how your information is collected, accessed and shared. We provide you with the means to make these choices.

41. Plaintiff and other Class Members relied to their detriment on Samsung's representations and were harmed by Samsung's omissions regarding data security, including Samsung's failure to alert customers that its security protections were inadequate and that Defendant would forever store the customers' PII, fail to archive it, fail to protect it, and fail to warn customers of the anticipated and foreseeable data breach.

42. Had Samsung disclosed to Plaintiff and Class Members that its data systems were not secure at all and were vulnerable to attack, Plaintiff would not have purchased Samsung's products or utilized its services that led to the account creation. Thus, Plaintiff and Class Members significantly overpaid based on what the products were represented to be compared to what Plaintiff and Class Members actually received.

43. To reduce the likelihood of data breaches like that which occurred here, the Federal Trade Commission ("FTC") has established security guidelines and recommendations for businesses like Samsung that possess their customers' sensitive PII. Among such recommendations are limiting the sensitive consumer information companies keep, encrypting

sensitive information sent to third parties or stored on computer networks, and identifying and understanding network vulnerabilities.

44. Thus, Samsung had obligations created by contract, industry standards, common law, and its privacy policies and representations to its customers to keep PII confidential and protect it from unauthorized disclosures exactly like that which occurred in the Data Breach.

45. Samsung enriched itself through the collection of a treasure trove of sensitive PII from Plaintiff and Class Members and profited from the collection, yet it failed to use some of those profits to employ reasonable, accepted safety measures to secure this valuable information.

SAMSUNG'S VERY LIMITED DISCLOSURE OF THE DATA BREACH

46. On September 2, 2022, Samsung released a statement that its "U.S. systems" had be infiltrated in "late July 2022" by an "unauthorized third party" and PII including at least customer names, contact, and demographic information, date of birth and product registration information had been stolen.

47. According to Samsung, the breach was not discovered until "around August 4, 2022" after an "ongoing investigation." Samsung did not disclose the breach to the affected customers for almost a month.

48. Samsung's carefully worded statement did not explain how the data breach occurred; how the breach was discovered; what systems were affected; why it took almost a month to disclose the breach; the number of Samsung customers affected; how long the investigation had been ongoing; the number of years of data involved; the volume of data accessed; what specific demographic data was stolen; the exact extent of the PII that was stolen; or whether this Data Breach was related to an earlier data breach of Samsung internal data.

49. Cybersecurity industry experts viewed the statement that was issued late on a Friday evening before the Labor Day holiday weekend, the failure to disclose the number of individuals impacted by the breach, and the month-long delay, as Samsung's attempt to minimize the incident.

SAMSUNG'S HISTORY OF DATA BREACHES

50. On March 7, 2022, Samsung announced it had suffered a data breach that exposed only internal company data, including the source code related to its Galaxy smartphones, algorithms related to Samsung smartphone biometric authentication, bootloader source code to bypass some of Samsung's operating system controls, source code for Samsung's activation servers and full source for technology used for authorizing and authenticating Samsung accounts.

51. Samsung claimed that the data breach did not include the PII of consumers or Samsung employees.

52. The breach came to light after the hacking group Lapsus$ disclosed 190GBs of Samsung's data to 400 peers.

53. Following the data breach, Samsung promised that it would implement measures to prevent further incidents and would continue to serve its customers without disruption.

54. It is possible that the Data Breach announced on September 2, 2022 is a continuation of the data breach announced on March 7, 2022. Given the difficulty of completely eliminating malware once it has infiltrated a network as large and complex as Samsung's, and the delay in disclosing the breach to the public, cybersecurity industry expert Chad McDonald has expressed the opinion that "this was quite likely just a continuation of [the earlier breach] they just hadn't discovered yet."

DATA BREACHES LEAD TO IDENTITY THEFT

55. Plaintiff and other Class Members have been injured by the disclosure of their PII in the Data Breach.

56. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[1] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

57. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconvenience repairing damage to their credit records" and their "good name."[2]

58. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

59. There may be a time lag between when PII is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft.* Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years.*

[1] *See* Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), United States Government Accountability office, available at httsp://www.gao.gov/new.items/d07737.pdf.

[2] *Id*. at 2, 9.

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

60. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[4]

61. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other PII directly on various Internet websites making the information publicly available.

CLASS ALLEGATIONS

62. Under Rule 23, Plaintiff brings this case as a class action on behalf of a Nationwide Class, and a Florida Sub-Class, defined as follows**:**

> Nationwide Class: All persons in the United States whose PII was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

---

[3] *Id*. at 29 (emphasis supplied).

[4] *See Federal Trade Commission,* WARNING SIGNS OF IDENTIFY THEFT, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

> Florida Sub-Class: All persons in the State of Florida whose PII was maintained on the Samsung systems that were compromised as a result of the breach announced by Samsung on or around September 2, 2022.

63. Excluded from the Classes are the following individuals and/or entities:

> Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

64. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

65. Numerosity, Rule 23(a)(1): The Nationwide Class and Florida Subclass ("Classes") are so numerous that joinder of all members is impracticable. Defendant has identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

66. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

67. Commonality, Rule 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated its common law duties to Plaintiff and Class Members by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages and/or punitive damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach;

m. Whether Defendant violated the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 and Florida Deceptive and Unfair Trade Practices Act, § 501.201 *et seq.*;

n. Whether Defendant's data security systems prior to the Data Breach met the requirements of applicable laws and regulations;

o. Whether Defendant's data security systems prior to the Data Breach met industry standards;

p. Whether Plaintiff's and other Class Members' PII was compromised in the Data Breach; and

q. Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

68. Typicality, Rule 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance. Plaintiff suffered the same injury as Class Members—*i.e.*, upon information and belief, Plaintiff's PII was compromised in the Data Breach.

69. Ascertainability: The Class and Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Class and Subclass consist of individuals who provided their PII to Samsung. Class Membership can be determined using Samsung's records and investigation.

70. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

71. Adequacy, Rule 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the proposed Classes. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members.

72. Defendant has engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

73. Superiority and Manageability, Rule 23(b)(3): A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendant. Concentrating this litigation in this forum is desirable to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendant's records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove the Plaintiff's claims and the Class Members' claims.

74. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

75. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

76. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

77. A class action is appropriate under Rule 23(b)(2) because Defendant has acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

78. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests. These particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant breached its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately, and accurately informed Plaintiff and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

f. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CLAIMS FOR RELIEF

COUNT I

Negligence
(On Behalf of Plaintiff and the Nationwide Class)

79. Plaintiff re-alleges and incorporates all of the allegations contained in the preceding paragraphs.

80. To access features of the devices, application or service that Plaintiff and Class Members purchased, Samsung required Plaintiff and Class Members to submit certain PII, including their names, dates of birth, email addresses and mailing addresses.

81. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

82. By collecting and storing this PII and using it for commercial gain, Samsung has both a duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and guard against theft of the PII.

83. Defendant knows of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

84. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using its customers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

85. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

86. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

87. Defendant's duty of care arose as a result of, among other things, the special relationship that existed between Samsung and its customers. Defendant was in a position to ensure that the PII of Plaintiff and Class Members was secure and that it was safeguarding and

protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

88. Defendant was subject to an "independent duty," untethered to any contract between Samsung and Plaintiff or Class Members.

89. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class Members was reasonably foreseeable to Defendant, particularly in light of Defendant's inadequate security practices and previous breach incidents.

90. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

91. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth here. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendant.

92. Plaintiff and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

93. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

94. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how

it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

95. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

96. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

97. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

98. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

99. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

101. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

102. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

103. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

104. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services that Plaintiff and Class Members received.

105. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II

Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff re-alleges and incorporates all of the allegations contained in the preceding paragraphs.

107. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

108. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep their PII contained and, as a part thereof, confidential.

109. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

110. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, through Defendant's failure to protect the PII.

111. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

112. The intrusion was into a place or thing that was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their use of Defendant's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their

belief that such information would be kept private and would not be disclosed without their authorization.

113. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

114. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with knowledge that its information security practices were inadequate and insufficient.

115. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

116. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

117. Unless enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT III

Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

118. Plaintiff re-alleges and incorporates all of the allegations contained in the preceding paragraphs.

119. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

120. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members due to the valuable nature of the PII at issue.

121. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

122. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

123. The harm that resulted from the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

124. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to, (i) actual identity

theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, or theft of their PII; (iv) out-of-pocket expenses associated with the prevention and detection of and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services Plaintiff and Class Members received.

125. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IV

Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff re-alleges and incorporates all of the allegations contained in the preceding paragraphs.

127. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transactions and should have been entitled to have Defendant protect their PII with adequate data security.

128. Defendant knew that Plaintiff and Class Members conferred a benefit on Defendant and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiff and Class Members for business purposes.

129. The amounts Plaintiff and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiff's and Class Members' PII.

130. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

131. Defendant failed to secure the PII of Plaintiff and Class Members and thus did not provide full compensation for the benefit Plaintiff and Class Members provided.

132. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

133. If Plaintiff and Class Members knew that Defendant would not secure their PII using adequate security, they would not have made purchases or provided their PII to Defendant.

134. Plaintiff and Class Members have no adequate remedy at law.

135. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to, (i) actual identity theft;

(ii) the loss of the opportunity to determine how their PII is used; (iii) the compromise, publication, or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services Plaintiff and Class Members received.

136. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

137. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from Plaintiff and Class Members. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's goods and services.

COUNT V

Violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1
(On Behalf of Plaintiff and the Nationwide Class)

138. Plaintiff realleges and incorporates by reference each allegation set forth above.

139. Plaintiff and all Class Members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

140. Defendant is a "person" as defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

141. Defendant's conduct as alleged here related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

142. Defendant advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of New Jersey.

143. Defendant solicited Plaintiff and Class Members to do business and uniformly and knowingly misrepresented that by opening a "Samsung Account," their PII was safe, confidential and protected from intrusion, hacking or theft.

144. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII by implementing and maintaining reasonable security measures.

145. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

146. Defendant failed to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

147. Defendant failed to provide notice to Plaintiff and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

148. Defendant's acts and omissions, as set forth here, evidence a lack of good faith, honesty in fact and observance of fair dealing, to constitute unconscionable commercial practices, in violation of N.J.S.A. 56:8-2.

149. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class Members are required to expend sums to protect and recover their PII, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII, and thereby suffered ascertainable economic loss.

150. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT VI

Violation of the Florida Deceptive and Unfair Trade Practices Act, § 501.201 et seq., Fla. Stat. ("FDUTPA") (On Behalf of Plaintiff and the Florida Subclass)

151. Plaintiff realleges and incorporates by reference each allegation set forth above.

152. Plaintiff and the Florida Subclass Members are "consumers" who used their credit cards to make payments to Samsung. *See* § 501.203(7), Fla. Stat.

153. The FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." § 501.204, Fla. Stat.

154. Samsung, by failing to inform consumers (including Plaintiff and the Florida Subclass Members) of its unsecure, non-compliant, and otherwise insufficient data and information security practices, advertised, sold, serviced, and otherwise induced those consumers to purchase goods and services from Samsung.

155. Samsung knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Florida Subclass Members' PII, and that the risk of a data breach was highly likely.

156. Samsung should have disclosed this information regarding its computer systems and data security practices because Samsung was in a superior position to know the facts related to its defective data security.

157. Florida law requires notification of data breaches upon identification. Upon information and belief, Samsung identified the Data Breach as early as July 2022, but only notified consumers on September 2, 2022, and therefore left those consumers at risk for the months in between discovery and notification.

158. Samsung's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Florida Subclass Members) regarding the security of its network and aggregation of PII.

159. The representations on which consumers (including Plaintiff and Florida Subclass Members) relied were material representations (*e.g.*, as to Samsung's adequate protection of PII), and consumers (including Plaintiff and Florida Subclass Members) relied on those representations to their detriment.

160. Samsung employed these false representations to promote the sale of a consumer good or service, which Plaintiff and Florida Subclass Members purchased.

161. As a direct and proximate result of Samsung's unconscionable, unfair, and deceptive acts or practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and damages as prescribed by § 501.211(2), Fla. Stat., including attorneys' fees.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23 and appointment of Plaintiff as Class Representative and his counsel of record as Class Counsel;

B. That the acts alleged herein be adjudged and decreed to constitute negligence and violate the consumer protection laws of the States of New Jersey and Florida;

C. A judgment against Defendant for the damages sustained by Plaintiff and the Classes defined here, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An award to Plaintiff and Class Members of pre-judgment and post-judgment interest as provided by law, and at the highest legal rate from and after service of the Complaint;

E. The costs of this suit, including reasonable attorneys' fees; and

F. Any other relief that the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, requests a jury trial, under Federal Rule of Civil Procedure 38, on all claims so triable.

Dated: September 27, 2022

Respectfully submitted,

/s/ *Mary L. Russell*
Mary L. Russell (NJ-0525119955)
Roberta D. Liebenberg (*pro hac vice* application forthcoming)
Gerard A. Dever (*pro hac vice* application forthcoming)
FINE, KAPLAN AND BLACK, R.P.C.
One South Broad Street, 23rd Floor
Philadelphia, PA 19107
Tel: (215) 567-6565
mrussell@finekaplan.com
rliebenberg@finekaplan.com
gdever@finekaplan.com

Counsel for Plaintiff and the Proposed Classes

Pursuant to Local Civil Rule 11.2, I hereby certify that the matter in controversy relates to the following civil actions:

- *Naeem Seirafi, et al. v. Samsung Electronics America, Inc.*, Civil Action No. 4:22-cv-01576 (N.D. Cal.), filed September 10, 2022;
- *Roald Mark v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-07974 (S.D.N.Y.), filed September 19, 2022; and
- *Harmer v. Samsung Electronics America, Inc.*, Civil Action No. 2:22-cv-01437 (D. Nev.), filed September 6, 2022.
- *Angela Robinson v. Samsung Electronics America, Inc*., Civil Action No. 1:22-cv-05722 (D.N.J.), filed September 26, 2022
- *Andrew Becker v. Samsung Electronics America, Inc*., Civil Action No. 2:22-cv-05723 (D.N.J.), filed September 26, 2022

- *Stephen Clark v. Samsung Electronics America, Inc.*, Civil Action No. 2:22-cv-05697 (D.N.J.), filed September 23, 2022

- *Athony Dipaola, et al. v. Samsung Electronics America, Inc.*, Civil Action No. 1:22-cv-05724 (D.N.J.), filed September 26, 2022

I hereby certify that the above statements are true. I am aware that if any of the foregoing statements made by me are willfully false, I am subject to punishment.

Dated: September 27, 2022

/s/ *Mary L. Russell*

Mary L. Russell (NJ-0525119955)
Roberta D. Liebenberg (*pro hac vice* application forthcoming)
Gerard A. Dever (*pro hac vice* application forthcoming)
FINE, KAPLAN AND BLACK, R.P.D.
One South Broad Street, 23rd Floor
Philadelphia, PA 19107
Tel: (215) 567-6565
mrussell@finekaplan.com
rliebenberg@finekaplan.com
gdever@finekaplan.com

Counsel for Plaintiff and the Proposed Classes